What is claimed is:

1. A method comprising:

receiving an ephemeral value from a challenging device;

retrieving data whose content is known to the challenging device;

generating a digital signature of the data based on the ephemeral value; and

transmitting the digital signature to the device.

2. The method of claim 1, wherein receiving the ephemeral value from the challenging device comprises receiving a randomly generated number from the challenging device.

3. The method of claim 1, wherein retrieving the data comprises retrieving at least part of application code.

4. The method of claim 1, wherein generating the digital signature of the data based on the ephemeral value comprises generating a one-way hash across the data based on the ephemeral value.

5. A method comprising:

receiving, into a response device, an ephemeral value from a challenge device;

retrieving data from an address space in the response device, wherein the data is known to the challenge device and the response device;

generating a hash across the data using the ephemeral value as a key of the hash; and

transmitting at least part of the hash to the challenge device.

6. The method of claim 5, further comprising generating a reduced hash based on the hash, wherein transmitting the ephemeral value and the at least part of the hash to the challenge device comprises transmitting the ephemeral value and the reduced hash to the challenge device.

7. The method of claim 5, wherein retrieving the data from the address space in the response device comprises retrieving application code to be executed in the response device.

8. The method of claim 5, wherein retrieving the data from the address space in the response device comprises retrieving configuration parameters of the response device.

9. A method comprising:

authenticating data having predictable content and stored in an address space of a remote device, the authenticating comprising:

generating a random number;

transmitting the random number to a remote device presumably having the data;

receiving, from the remote device, a first digital signature that is representative of the data;

generating a second digital signature based on the random number; and

comparing the first digital signature to the second digital signature.

10. The method of claim 9, wherein authenticating the data having predictable content comprises authenticating an application executable.

11. The method of claim 9, wherein authenticating the data having predictable content comprises authenticating at least one security parameter.

12. The method of claim 9, wherein authenticating further comprises marking the data as authenticated if the first digital signature equals the second digital signature.

13. An apparatus comprising:

a storage medium to store data;

an input/output (I/O) logic to receive a request for authentication, wherein the request includes an ephemeral value; and

a signature logic to retrieve at least part of the data from the storage medium and to generate a cryptographic hash across the at least part of the data based on the ephemeral value.

14. The apparatus of claim 13, wherein the I/O logic is to receive the request for authentication from a challenge device, the I/O logic to transmit the cryptographic hash back to the challenge device.

15. The apparatus of claim 13, wherein the storage medium is a nonvolatile memory.

16. The apparatus of claim 13, further comprising a data selection logic to select less than all of the data, wherein the at least part of the data is the less than all of the data.

17. The apparatus of claim 16, wherein the data selection logic is to select less than all of the data based on a random number based selection of segments of the data.

18. The apparatus of claim 13, wherein the data comprises an application to be executed in the apparatus.

19. The apparatus of claim 13, wherein the data comprises at least one security parameter of the apparatus.

20. A challenge device to authenticate data presumably stored in a response device, the challenge device comprising:

a storage medium to store a copy of the data presumed to be stored in the response device;

a key generation logic to generate an ephemeral value;

an input/output (I/O) logic to output a request for authentication to a response device, wherein the request includes the ephemeral value, the I/O logic to receive a first digital signature from the response device in response to the request for authentication;

a signature logic to retrieve the copy of the data and the ephemeral value and to generate a second digital signature; and

an authentication logic to compare the first digital signature to the second digital signature, wherein the data is authenticated if the first digital signature equals the second digital signature.

21. The challenge device of claim 20, wherein the ephemeral value comprises a randomly generated value.

22. The challenge device of claim 20, wherein the data comprises application code to be executed by the response device.

23. The challenge device of claim 20, wherein the data comprises at least one configuration parameter of the remote device.

24. A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

receiving an ephemeral value from a challenging device;

retrieving data whose content is presumed known to the challenging device;

generating a digital signature of the data based on the ephemeral value; and

transmitting the digital signature to the device.

25. The machine-readable medium of claim 24, wherein receiving the ephemeral value from the device comprises receiving a randomly generated value from the device.

26. The machine-readable medium of claim 24, wherein retrieving the data comprises retrieving at least part of application code.

27. The machine-readable medium of claim 24, wherein generating the digital signature of the data based on the ephemeral value comprises generating a one-way hash across the data based on the ephemeral value.

28. A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

receiving, into a response device, an ephemeral value from a challenge device;

retrieving data from an address space in the response device, wherein the data is presumed known to the challenge device;

generating a hash across the data using the ephemeral value as a key of the hash; and

transmitting at least part of the hash to the challenge device.

29. The machine-readable medium of claim 28, further comprising generating a reduced hash based on the hash, wherein transmitting the ephemeral value and the at least part of the hash to the challenge device comprises transmitting the ephemeral value and the reduced hash to the challenge device.

30. The machine-readable medium of claim 28, wherein retrieving the data from the address space in the response device comprises retrieving application code to be executed in the remote device.

31. The machine-readable medium of claim 28, wherein retrieving the data from the address space in the response device comprises retrieving configuration parameters of the remote device.

32. A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

authenticating the data having predictable content and stored in an address space of a remote device, the authenticating comprising:

generating a random number;

transmitting the random number to a device presumably having the data;

receiving a first digital signature that is representative of the data;

generating a second digital signature based on the random number; and

comparing the first digital signature to the second digital signature.

33. The machine-readable medium of claim 32, wherein authenticating the data having predictable content comprises authenticating an application executable.

34. The machine-readable medium of claim 32, wherein authenticating the data having predictable content comprises authenticating at least one security parameter.

35. The machine-readable medium of claim 32, wherein authenticating further comprises marking the data as authenticated if the first digital signature equals the second digital signature.